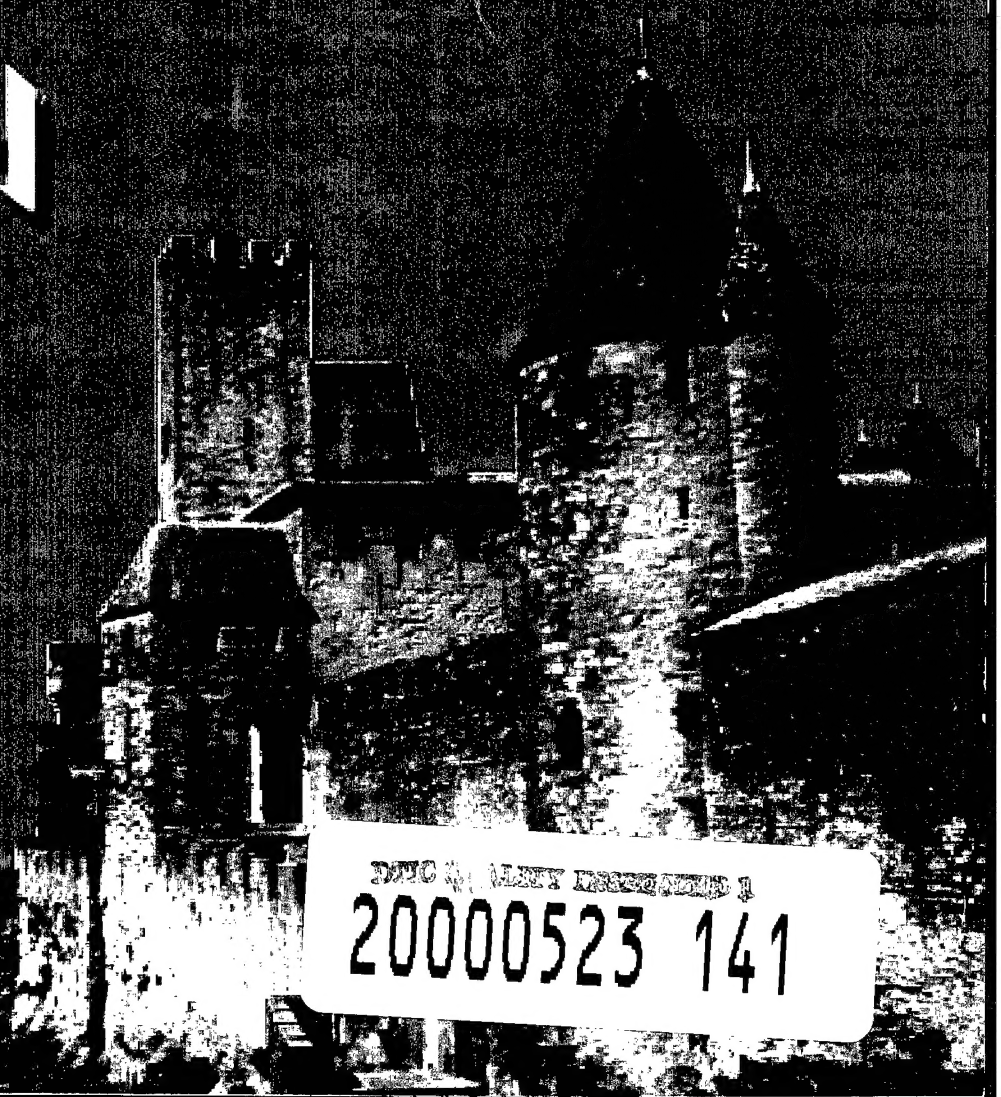
Information Assurance Through DEFENSE IN DEPTH

February 2000



From The J6 –

Throughout history, successful military operations have depended upon timely and accurate information. In the age of digital electronics, our forces rely upon computers and telecommunications as essential information capabilities that are being networked into a complex, massive Global Information Grid (GIG). The GIG is vital to achieving Information Superiority—the key enabler to achieving the Joint Vision 2010 goal of Full Spectrum Dominance. The organizational and procedural framework to manage the GIG is provided by Network Operations (NETOPS).

Because these information capabilities are so valuable as weapons, they are also lucrative targets that are under threat of harm in all national security situations from peacetime through full-scale war. In this environment of danger, where every connection to a network must be regarded as a potential threat avenue of approach, we must conduct Information Operations (IO) to defend our own information and information systems and to affect adversary information and information systems that can be used against us. Information Assurance (IA) is a major subset of Information Operations that includes measures to protect and defend at the tactical, operational, and strategic levels. NETOPS integrates Information Assurance with Network Management and Information Dissemination Management (IDM). The Information Assurance challenges before us are clearly and sharply evident.

We can and will prevail over these challenges through a **DEFENSE IN DEPTH** approach to Information Assurance. **DEFENSE IN DEPTH** integrates the capabilities of people, operations, and technology to achieve strong, effective, multi-layer, multi-dimensional protection.

This publication is our first venture in a projected series intended to assist and guide those who defend our computers and computer networks. We seek a wide readership for this brochure, and encourage and welcome constructive comment. **DEFENSE IN DEPTH** concepts are the way ahead and the benchmarks for strong and effective Information Assurance.

JOHN L. WOODWARD, JR.
Lieutenant General, USAF
Director for Command, Control, Communications and Computer Systems, The Joint Staff

DEFENSE TECHNICAL INFORMATION CENTER
REQUEST FOR SCIENTIFIC AND TECHNICAL REPORTS

Title Information assurance through Defense in Depth

1. Report Availability *(Please check one box)*

☑ This report is available. *Complete sections 2a - 2f.*

☐ This report is not available. *Complete section 3.*

2a. Number of Copies Forwarded

1

2b. Forwarding Date

17 May 00

2c. Distribution Statement *(Please check ONE box)*

DoD Directive 5230.24, "Distribution Statements on Technical Documents," 18 Mar 87, contains seven distribution statements, as described briefly below. Technical documents MUST be assigned a distribution statement.

☑ DISTRIBUTION STATEMENT A: Approved for public release. Distribution is unlimited.

☐ DISTRIBUTION STATEMENT B: Distribution authorized to U.S. Government Agencies only.

☐ DISTRIBUTION STATEMENT C: Distribution authorized to U.S. Government Agencies and their contractors.

☐ DISTRIBUTION STATEMENT D: Distribution authorized to U.S. Department of Defense (DoD) and U.S DoD contractors only.

☐ DISTRIBUTION STATEMENT E: Distribution authorized to U.S. Department of Defense (DoD) components only.

☐ DISTRIBUTION STATEMENT F: Further dissemination only as directed by the controlling DoD office indicated below or by higher authority.

☐ DISTRIBUTION STATEMENT X: Distribution authorized to U.S. Government agencies and private individuals or enterprises eligible to obtain export-controlled technical data in accordance with DoD Directive 5230.25, Withholding of Unclassified Technical Data from Public Disclosure, 6 Nov 84.

2d. Reason For the Above Distribution Statement *(in accordance with DoD Directive 5230.24)*

Document is unclassified, not sensitive and intended for public release.

2e. Controlling Office

JCS/J6K

2f. Date of Distribution Statement Determination

17 May 00

3. This report is NOT forwarded for the following reasons. *(Please check appropriate box)*

☐ It was previously forwarded to DTIC on ____________ *(date)* and the AD number is ____________

☐ It will be published at a later date. Enter approximate date if known. ____________

☐ In accordance with the provisions of DoD Directive 3200.12, the requested document is not supplied because: ____________

Print or Type Name

Patrick W. Phillips

Signature

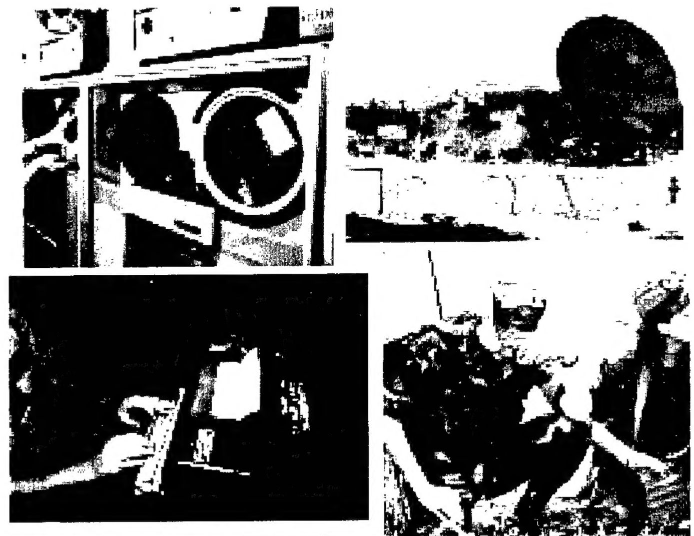
Telephone

[illegible]

(For DTIC Use Only)

AQ Number

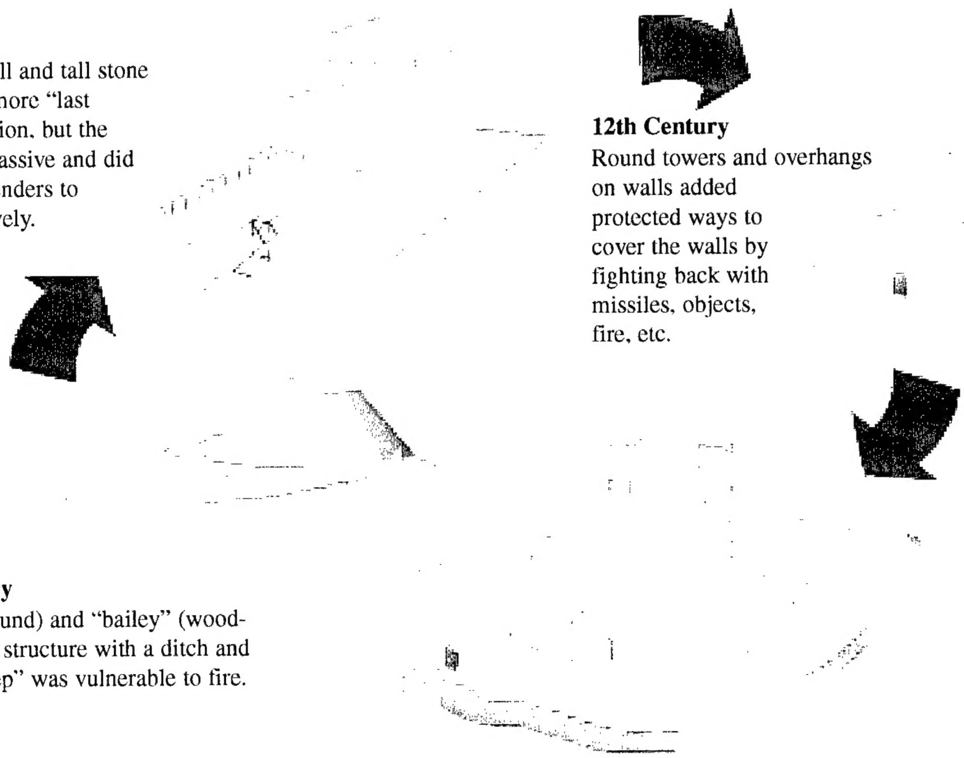
Information Assurance



Digital electronic systems are vital to our military operations

Our armed forces increasingly rely on critical digital electronic information capabilities to store, process, and move essential data in planning, directing, coordinating, and executing operations. Powerful and sophisticated threats (circumstances or events that can cause unauthorized access, destruction, disclosure, modification of data, or denial of service) can exploit security weaknesses in many of these systems. Weaknesses that can be exploited become vulnerabilities that can jeopardize the most sensitive components of information capabilities. However, we can employ deep, layered defenses to reduce vulnerabilities and deter, defeat, and recover from a wide range of threats.

This brochure describes how to achieve **Information Assurance (IA)** for digital electronic information capabilities through **DEFENSE IN DEPTH**. It describes the principal components and layers of our endangered systems and threats against them, the concept of **DEFENSE IN DEPTH**, and the contributions of people, operations, and technologies that defend the layers.



11th Century
"Motte" (mound) and "bailey" (wood-fenced yard) structure with a ditch and wooden "keep" was vulnerable to fire.

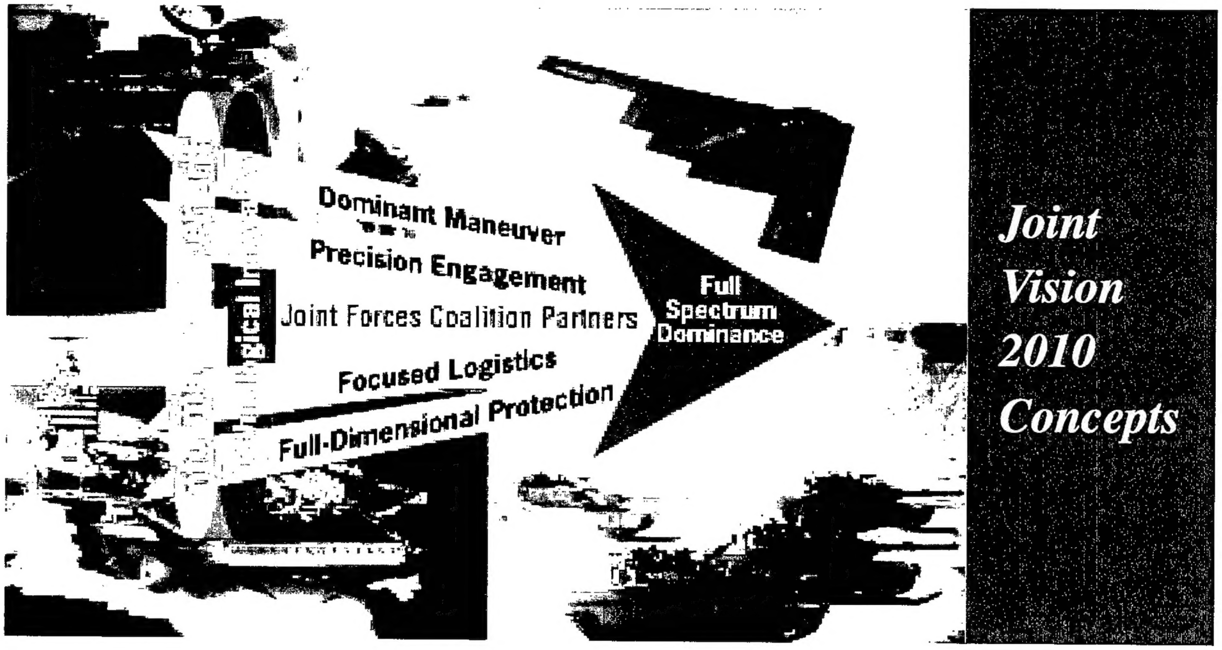
12th Century
A "curtain" wall and tall stone "keep" added more "last refuge" protection, but the keep was too passive and did not enable defenders to fight back actively.

12th Century
Round towers and overhangs on walls added protected ways to cover the walls by fighting back with missiles, objects, fire, etc.

13th Century
A second curtain wall, wet ditch, crosswalls, slotted walls (crenelation), and strong gatehouse added more barrier layers to extend the depth of defense.

The dynamically evolving defenses of the medieval castle offer a valuable analogy

In that violent age, castles offered secure bases for armed forces to control key terrain. In response to changing threats, they evolved from simple to complex and very strong fortifications, following **two principles: (1) increase and strengthen the defensive barriers, and (2) provide means to fight back actively**. Castles on strong foundations, often on higher ground, employed successive barriers such as water obstacles, ditches, rings of strong and high walls with overhangs, and towers. Improvements to the walls allowed defenders to engage the attacker, and multiple gates enabled local counterattacks and raids. A small force could hold out against a much larger adversary. Just as the castle protected critical resources, now we must defend our vital military information and actively fight back with appropriate responses.



Information Superiority and Information Operations (IO)

Information Operations (IO) are operations conducted to defend our own information and information systems and affect adversary information and information systems. They are essential to achieving the ***Joint Vision 2010*** concept of **Information Superiority**—the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. Information Superiority is achieved through dominance in intelligence, command and control, communications, computers, and Information Operations (IO).

Information Assurance (IA)

Information Assurance (IA) is a subset of Information Operations (IO). Information Assurance (IA) is actions that protect and defend information and information systems by ensuring availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. (Source: U.S. Dept. of Defense, Joint Staff, Joint Publication 3-13 *Information Operations*, 9 October 1998.)

Security Attributes:

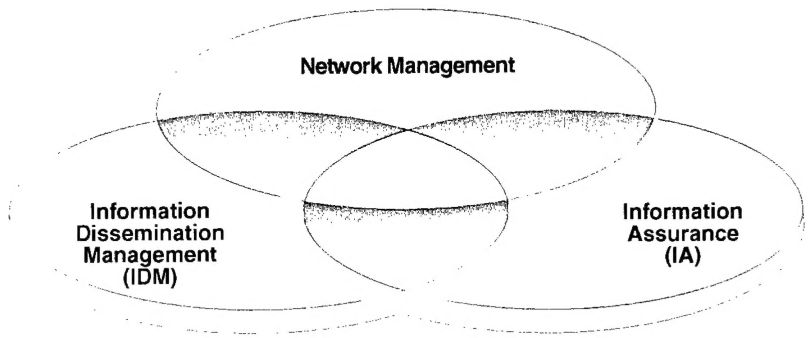
- **Availability**—Timely, reliable access to data and services for authorized users. Includes restoration.
- **Identification and Authentication**—Identification is the process an information system uses to recognize an entity. Authentication is a security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an authorization to receive specific categories of information.
- **Confidentiality**—Assurance that information is not disclosed to unauthorized persons, processes, or devices.
- **Integrity**—Protection against unauthorized modification or destruction of information.
- **Nonrepudiation**—The sender is provided with proof of delivery, and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data.

"[T]he amorphous nature of today's security environment means the threats will be far more difficult to anticipate and counter. These asymmetric threats pose end games that are still potentially devastating to countries and alliances. We must, individually and collectively, anticipate these types of threats and have the courage to deal with them."
—General Henry H. Shelton, Chairman, Joint Chiefs of Staff, "The Transatlantic Commitment" at "NATO at 50" conference, London, 08 March 1999.

Network Operations (NETOPS)

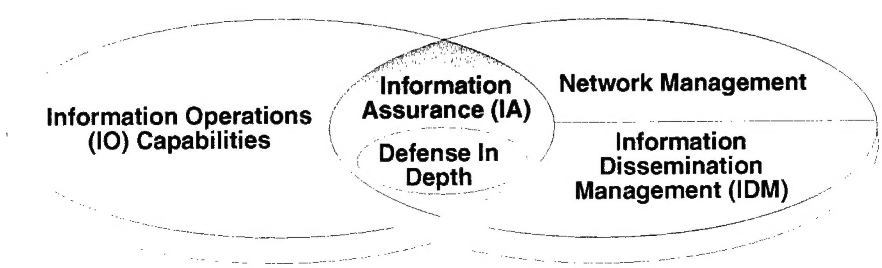
We must have agile and comprehensive awareness and control of our Global Information Grid (GIG) of networked systems in order to attain Information Superiority. Network Operations (NETOPS) will provide the organizational and procedural framework to manage the GIG and enable Commanders-in-Chief of Combatant Commands (CINCs) and other DOD components to apply Information Superiority to mission accomplishment. The NETOPS framework integrates the functions of:

- Network Management
- Information Dissemination Management (IDM)
- Information Assurance (IA)



Network Operations (NETOPS)

Information Dissemination Management (IDM) will prioritize the importance and delivery of information. Network Management will make visible the extent and intensity of activity, traffic load, and throughput potential. It will enable dynamic rerouting based on Information Dissemination Management priority, system status, and capacity. The effects of disruptions and intrusions will be minimized through allocation of traffic to unaffected available network paths. The **DEFENSE IN DEPTH** approach, tactics, techniques, and procedures are vital elements of Information Assurance, each commander's Information Operations concept of operations, and the overall NETOPS effort.



Information Operations Capabilities

Network Operations of the Global Information Grid

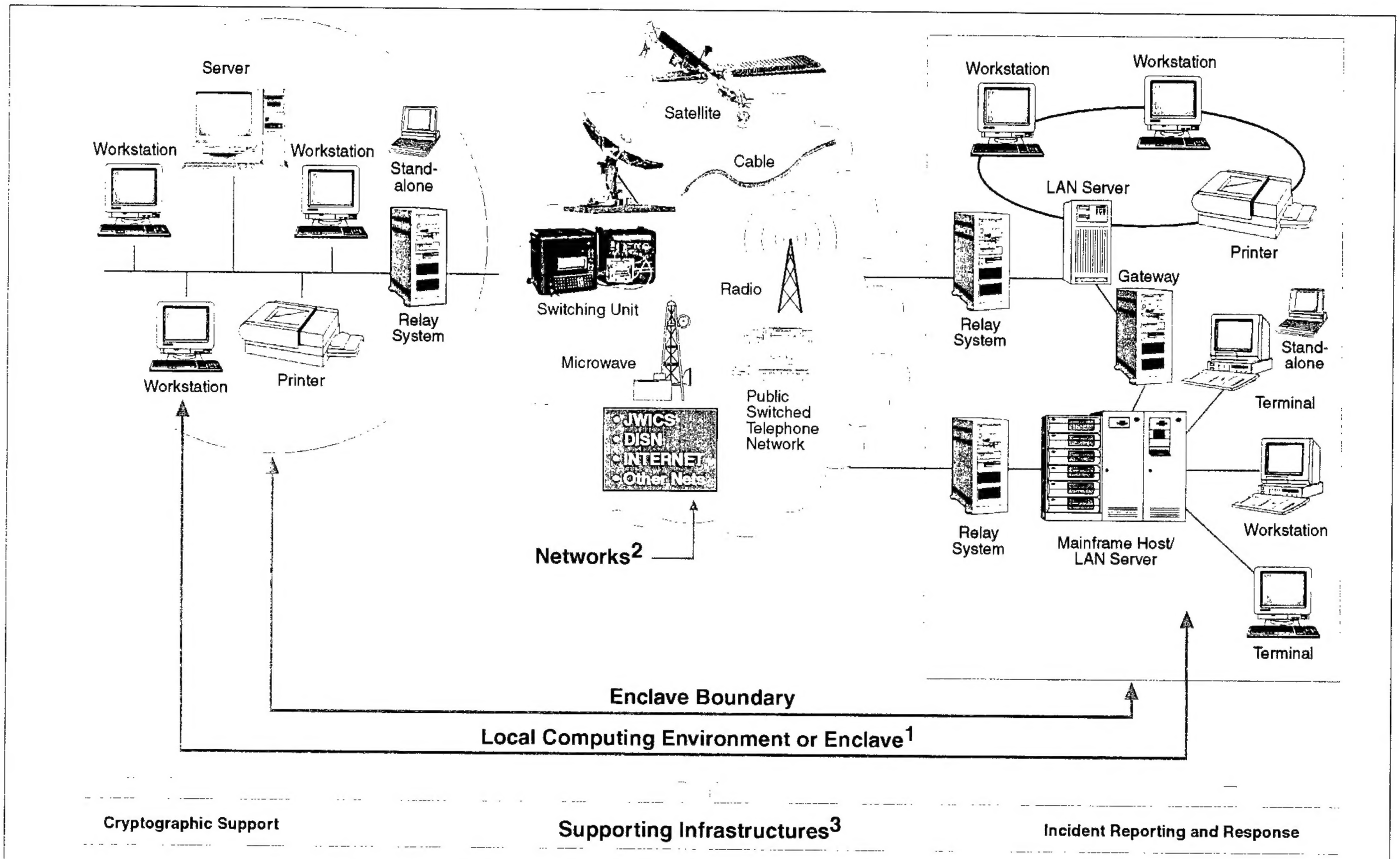
DEFENSE IN DEPTH is a Vital Element of NETOPS

The Information Environment

From an Information Assurance perspective, the capabilities that we must defend can be viewed broadly in terms of four major elements:

- **Local Computing Environments**, or **Enclaves**
- **Enclave Boundaries**
- **Networks** that link enclaves
- **Supporting Infrastructures**

The complex nature of the information environment is represented by the following illustration.



Major Elements of the Information Environment

1 ***Local Computing Environment (Enclave)***—The total physical and organizational environment, including all end-system devices and communications systems (such as relay systems) under control of a single authority with a common, uniform policy that governs security-related practices. Includes data, applications, people, and facilities.

- ***End-Systems***—Mainframe computers, terminals, workstations, printers, and storage devices. *End-systems have their own in-depth structure* of hardware and software components: communication elements, operating systems, applications software, mass storage, input peripherals, and output devices such as visual displays, printers, and plotters. Firmware (software embedded in a hardware device) can allow reading and executing the software, but not modifying.
- ***Local Area Network (LAN)***—Local interconnections of communications entities to provide telecommunications capabilities to transport data.
- ***Relay Systems***—Intermediary communications devices and capabilities such as multiplexers, routers, switches, or gateways. Connections to the networks are only through relay system functions.

2 ***Networks***—Networks to transport data and information between enclaves. Includes data, applications, people, and facilities.

- ***JWICS***—Joint Worldwide Intelligence Communications System.
- ***DISN***—Defense Information Systems Network. An integrated network that is centrally managed and configured to provide long-haul information transfer services for all Department of Defense (DOD) activities. It is designed to provide dedicated point-to-point, switched voice and data, imagery, and video teleconferencing services. Major components include: Secret Internet Protocol Router Network (SIPRNET) and Unclassified but sensitive Internet Protocol Router Network (NIPRNET).

3 ***Supporting infrastructures***—Organized capabilities to provide special support, such as cryptographic logistics.

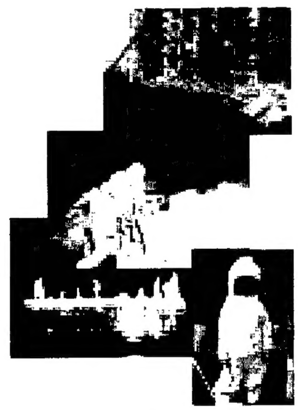
Threats

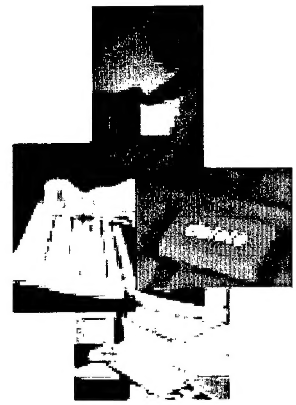
There are three basic sources of threats that alone or in combination can cause great damage if we are not prepared for them:

- Natural Environment
- Man-made Physical Hazards
- Human Actors

Natural environment threat sources spring from the elements and forces of raw nature: atmosphere (wind, natural chemicals and gases); water (rain, rising floods); earth (earthquake, mudslide, volcanic eruption and lava); electromagnetic and particle radiation/current (the sun and other cosmic sources, lightning, minerals); and fire.

Natural Environment


Man-made Physical Hazards


Human Actors

Man-made physical hazards would come from natural physical elements and forces that have been influenced or used (modified, rearranged into new "creations") by human action. These include: structures (e.g., collapse from construction or material weakness); mechanical devices, machines, tools, equipment; electromagnetic and particle radiation (fallout and emmissions from nuclear explosion or nuclear accident involving a power plant, a laboratory, transported materials); heat/ventilation/cooling/humidity control systems; water (from plumbing/fire suppression systems or leakage through structural weakness); hazardous and harmful chemicals and gases; blast, heat, and flame from explosives; theft.

Human actors pose the special danger of stealthy, widespread, sustained, penetrating, high-loss Computer Network Attack (CNA). We are under assault by a rogues gallery that includes: amateur hackers, foreign government organizations, spies, terrorists, officials acting unlawfully, business enterprises, other non-government and non-corporate organizational raiders, professional criminals, hostile insiders, and insiders who may cause mistakes or accidents.

Computer Network Attack (CNA)—Operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks or the computers and networks themselves:

- **Passive Intercept Attack**—Traffic monitoring, copying, analyzing, cryptographic decoding, and capturing identification (ID) numbers and passwords.
- **Active Network-Based Attack**—Attempts to circumvent or break security features, introduce malicious code or to steal or modify information. These include attacks mounted against a network backbone, exploitation of information in transit, electronic penetrations into an enclave, or attacks on an authorized remote user who is attempting to connect to an enclave.
- **Insider Attack**—Insiders are either authorized to be within the physical boundaries of the system or network or have authorized electronic access to that system or network. Malicious insiders can eavesdrop, steal, or damage information. They also can deny access by other authorized users. Non-malicious insiders can inflict accidental harm because of carelessness or lack of knowledge.
- **Hardware/Software Distribution Attacks**—Malicious modification of hardware or software at the factory, or modification or substitution during distribution.

A shared-risk environment is created when a vulnerable system connects to other systems that trust it to be secure and thereby exposes the other systems to harmful exploitation by threats. **DEFENSE IN DEPTH** must ensure that the level of protection of one system is not undermined by vulnerabilities of other interconnected systems.

DEFENSE IN DEPTH depends on people, operations, and technologies *working together at all layers* of the protected systems.

Defense in Depth

The **DEFENSE IN DEPTH** approach integrates the capabilities of **people**, **operations**, and **technology** to establish multi-layer, multi-dimension protection—like the defenses of a castle.

Constructing successive layers of defense will cause an adversary who penetrates or breaks down a barrier to promptly encounter another **DEFENSE IN DEPTH** barrier, and another, until the attack ends. A simple strategy of redundancy that uses the same method on successive barriers may not be effective against a variety of attack methods. To counter different attack methods, we must employ a corresponding **variety of security methods**. The weaknesses of one safeguard mechanism should be balanced by the strengths of another. To block threats to different locations in the protected environment, we must deploy our defenses at **multiple locations** on the layers. No critical sector or avenue of approach into the sensitive domains of the information system should be uncontested or unprotected.

"The best defense . . . is a lot of defense." —Frank Hayes, "Hacker Lessons: Frankly Speaking," *Computerworld,* 16 August 1999

There are four DEFENSE IN DEPTH areas of focus:

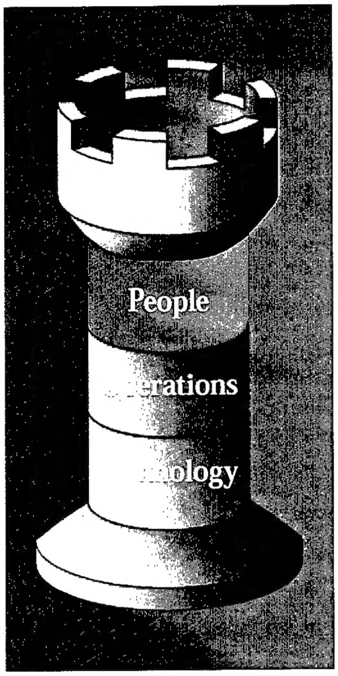
- **Local Computing Environments**, or **Enclaves**
- **Enclave Boundaries**
- **Networks** that link enclaves
- **Supporting Infrastructures**

We must prioritize our defensive efforts to get the maximum protective benefit from available resources. This can be accomplished by careful **risk analysis** that focuses on the value of information and systems, the likelihood of threats, and the nature and scope of potential harm. This analysis lays the foundation for **risk management**—selection and implementation of effective and affordable security mechanisms that meet prioritized security requirements. Any remaining exposure (residual risk) from uncovered vulnerabilities must be identified, evaluated and explained or justified in terms of operational impacts, and recorded.

A critical dimension of **DEFENSE IN DEPTH** is **time**. We cannot wait until systems are fielded before worrying about how to protect them. Instead, security safeguards must be designed-in before production. Post-deployment changes in missions, criticality, threats, and technologies demand continual attention and modifications. After they are implemented, security measures must work reliably around-the-clock.

Furthermore, the security measures must be **interoperable**. They must coexist in the same environment and not conflict with each other. They cannot impose unacceptable computing, communications, or organizational burdens or obstacles that hamper accomplishment of vital operations. They should work together in such functions as sharing data and providing cues, indications, or triggers to perform actions.

"Winning is not a sometime thing. It's an all the time thing." —Vince Lombardi

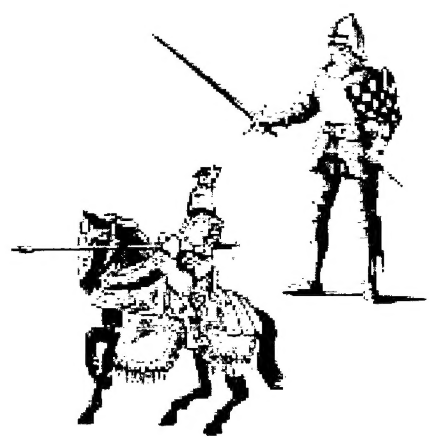


People

People, using technologies to conduct operations, are the central element of **DEFENSE IN DEPTH**. It takes people to design, build, install, operate, evaluate, and maintain protection mechanisms. To gain and maintain the knowledge and expertise to perform these vital tasks, a comprehensive program of **education**, **training**, practical **experience**, and **awareness** is needed. **Professionalization and certification** licensing can increase motivation and provide a validated, recognized, expert cadre.

We must **recruit** and wisely assign the best talent available. We also need a highly reliable **personnel security** system of appropriate background investigations, security clearances, credentials and badges, and attention to suspicious actions to ensure only trustworthy persons have access.

In modern defense forces, individual contributions must be integrated into larger coordinated team and organization efforts. **Command** attention, positive involvement, and **leadership** are vital at all levels of organization. Every person who uses or manages information systems has a responsible security role. Key **roles** include: commander or director, System Administrator (SA), Network Administrator (NA), Information Systems Security Manager (ISSM), Information Systems Security Officer (ISSO), Designated Approving Authority (DAA), and end-user. The following discussion of operations identifies important actions that are performed in these roles.



Castle sentries on towers and walls maintained a watch for attacks. Because treachery and stealth often were attempted to bring down a castle, those inside the fortification would be on the alert for suspicious activity by insiders. Networks of spies and informants and patrols would watch the networked lines of communication between fortified places.

Operations

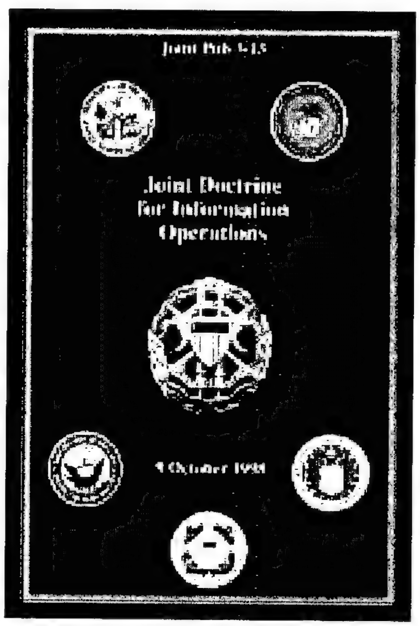
Information Assurance (IA) Policy drives IA operations by establishing goals, actions, procedures, and standards. Policy formally states the security requirements in terms of what must be protected, how resources are used, and what must be done and not done. Policy establishes standards that define uniform and common features and capabilities of security mechanisms, the rule or basis by which to measure the various dimensions of Information Assurance, and the desired or required level of attainment.

DEFENSE IN DEPTH requires three main types of policy:

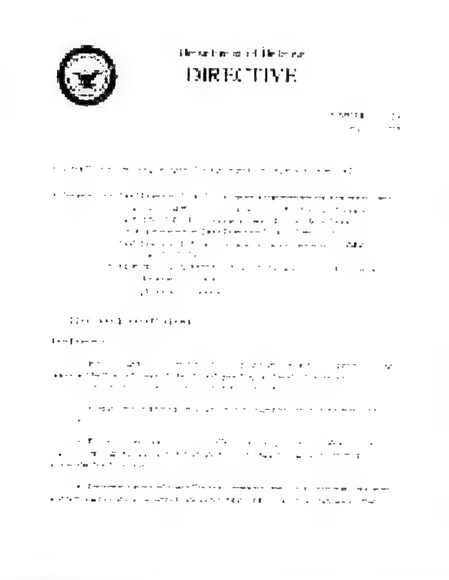
- ***Program policies***—Establish the organization's security effort in terms of: purpose, goals, scope, resource allocation, authorities and responsibilities, and compliance (violations and penalties).
- ***Issue-specific policies***—Specific issues, such as continuity of operations planning or Internet access.
- ***System-specific policie*s**—Objectives, rules, procedures and standards for specific systems.

Policies are issued at different levels of organization. At the national level, policies are established by legislation, judicial interpretations, and Executive Branch issuances from the President and authorized departments, agencies, and inter-organizational bodies. Federal agencies and departments formulate policies at their level. DOD policies include directives, instructions, regulations, manuals, and standards. **Military guidance** and doctrine for joint employment and activities of the Armed Forces are issued by the Chairman of the Joint Chiefs of Staff. **Doctrine** establishes fundamental principles to guide actions in support of national objectives. DOD agencies, Military Departments and Services, and subordinate organizations publish additional policies for their areas of responsibility.

Written **plans** document the policies and other important elements of the program. Plans should address: the architecture and configuration of the information capability, descriptions, assessments and audits, security measures and procedures, incident response, continuity of operations, personnel security, and training and awareness. **Standard operating procedures** (SOP) should define routine operations and incident response and reporting.


Joint Doctrine for Information Operations

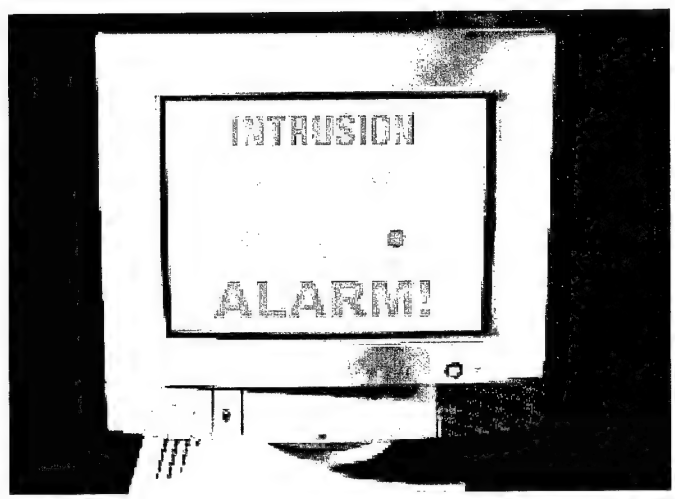
9 October 1998


DIRECTIVE

The basic doctrine for Information Assurance (IA) is stated in Joint Publication 3-13, ***Information Operations.*** Joint Publication 1-02, *DOD Dictionary of Military Terms,* affirms that doctrine is authoritative, but requires judgment in application. DOD Directive 5200.28 ***Security Requirements for Automated Information Systems (AISs)*** provides basic policy for the Department.

Expert, well-organized **monitoring, management, and administration** are required. We must carefully maintain comprehensive inventories and architecture descriptions. Diligence and skill are required to monitor vulnerability listings and implement fixes, ensure security mechanisms are interoperable, keep a constant watch over the security situation and mechanisms, properly employ and upgrade tools and techniques, and deal rapidly and effectively with issues.

Intelligence and **indications and warning** provide invaluable advance understanding of potential threats and notice of attack. If attack occurs, **DEFENSE IN DEPTH** also requires a widely distributed **intrusion detection** effort to recognize and describe activities that are different from the normal pattern or fit known "bad" patterns. The nature and scope of the incident, effects, cause, and vulnerability must be determined.



After an intrusion is detected, **incident information must be reported** through established channels to appropriate authorities and specialized analysis and response centers. **Incident response** begins with immediate local emergency damage-limitation and survivability actions that should be stated in the SOP and implemented promptly. Regional and national experts may need to get involved with more sophisticated methods to confirm attacks, determine effects, and track down perpetrators. These tasks may be quite difficult when distributed, coordinated, low-visibility network-based attacks occur across many systems over an extended period of time. Careful, effective, and timely decisions must be made concerning appropriate additional responses, such as: declare a higher level security situation or information operations condition (INFOCON), isolate affected elements, or pursue legal, diplomatic, economic, or military actions. Skillfully integrated Information Operations (IO) counterattack or counteroffensive actions can contribute significantly to the overall defensive effort, in the same way that sorties and raids aided in the defense of a castle.

Defense of a castle demanded the sustained, organized, and integrated operations of combatants and other occupants, who provided vital support. Everyone was vigilant and ready to respond to alarms of attack and actively fight back. Resolute leadership and careful management of available resources were needed to defeat the adversary's attempt to seize the castle.

Response measures must also ensure that information systems essential to performing critical missions are not crippled by unacceptable interruption. **Continuity Of Operations Plan (COOP)** and **Critical Asset Assurance Program (CAAP)** actions counter significant loss of critical assets and operations by providing means to keep functioning and achieve subsequent restoration.

COOP Phases:

- **Preparatory or pre-event** measures prioritize functions and assets in relation to time. Regular backup copies of critical files and applications and arrangements for alternate resources are vital. Training and testing prepare the people.
- **Trans-event** actions focus on military functions.
- **Post-event actions** restore military operations, then other functions in priority.

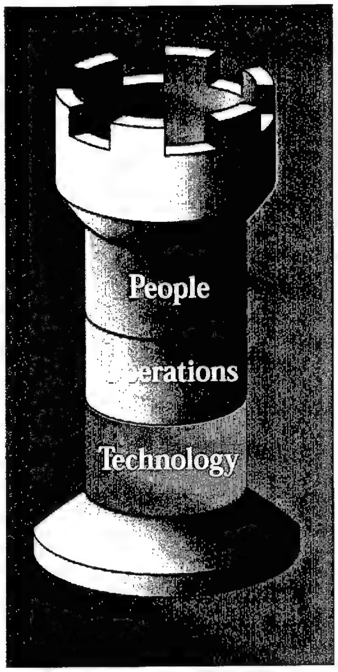
Assessments and audits by internal and outside evaluators are necessary to obtain a clear and accurate understanding of the actual IA readiness situation. To gain this knowledge, program reviews evaluate organization, resources, and policies. Technology tools, such as automated scanners for networks and end-items and components, can assist in vulnerability assessments. An independent audit offers a valuable examination of records and activities to assess adequacy of controls and compliance with policies and procedures. Penetration tests ("red team" activities) offer unique insights beyond what is gained from examination of records. Independent evaluations can add new information and validate previous assessments.

When disaster strikes . . . continue and restore

Within DOD, assessment is a key element in the **certification and accreditation (C&A)** process to obtain official authorization to operate a system. The DOD Information Technology Security Certification and Accreditation Process (DITSCAP) requires systematic and comprehensive risk analysis and risk management, with documented assessments and security measure decisions. C&A are conducted on a periodic basis and when there are significant system changes.

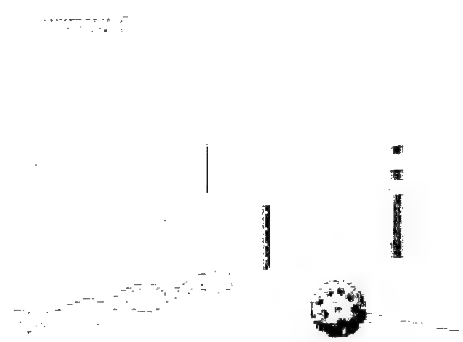
In the shared risk environment, we must ensure that enclaves and other systems seeking access to the networks do not expose other enclaves to their vulnerabilities. A formal **process for approving connections** to designated networks is vital to accomplishing this task by requiring certain security features and procedures.

DEFENSE IN DEPTH operations rely on the basic features and capabilities of the end-items and components, as well as an increasing array of effective technology tools to deploy across layers of the protected architecture. The following section describes these tools, as well as the special supporting infrastructures.



Technology

To conduct an effective cyber-defense, we must have a well-stocked arsenal of technological weapons and the skills to use them. We can have greater confidence in the effectiveness of the technology tools and products used in DOD Information Assurance (IA) solutions when they have been evaluated under programs conducted by the members of the National Information Assurance Partnership (NIAP) framework. NIAP was established by a 1997 agreement between the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA).

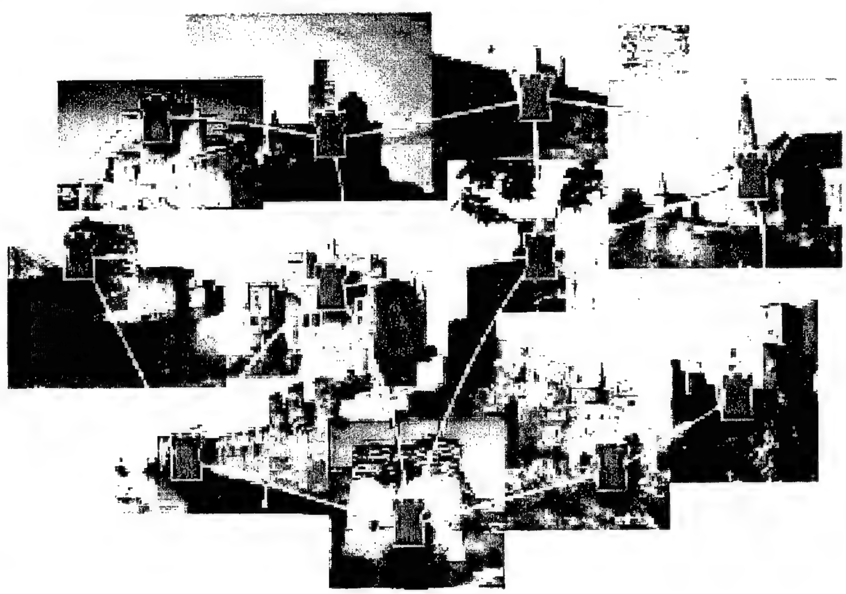


Technology to Defend the Networks

We must protect the vital lines of electronic communication that link our enclaves. Some important technologies to help defend these networks include:

- **Redundant and multiple data paths** offer more than one available alternate physical medium or route for data transport. These measures serve to ensure continued transmission when intermediate enclaves or network components are degraded or inoperable. Enclaves should be able to disconnect from external networks in a crisis, filter traffic to prevent the use of risky message segments, and control throughput. Provisions against denial of service should be included in agreements for commercial services, such as public switched networks. In addition, services should be procured from more than one source—to avoid a single point of failure.

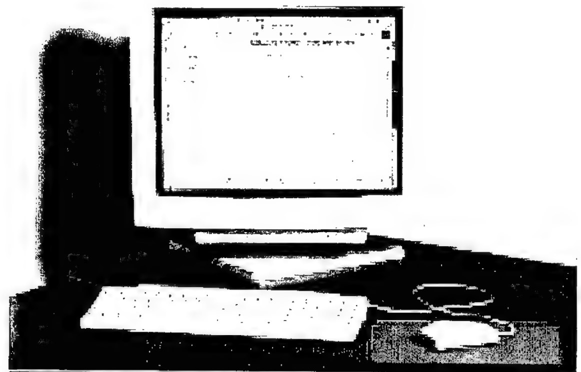
Castle defenses would use every available means of defense. In addition to walls, outer obstacles in the form of water moats or dry ditches would impede attackers. Such physical measures would be complemented by armed fighters employing arrows, spears, swords, axes, clubs, pikes, flung rocks, and hot or burning liquids.



"The instruments of battle are valuable only if one knows how to use them."
—Ardant du Picq, *Battle Studies*

Medieval castles had to maintain a security watch over vital supply and movement routes against bandits and invaders. Active military operations by armed patrols and larger forces were often needed to eliminate the threat. Messages sent between rulers were protected by codes and armed guards.

- Automated tools for **monitoring and management** should be employed on the networks to collect and analyze observable phenomena and maintain knowledge of the network status. These tools should be able to detect disruption and degradation that can indicate security problems.
- Manual methods lack the capacity to check all incoming traffic for attacks, or to inspect all the records of all user activities. Automated tools are necessary. Widely-deployed **intrusion detection** instrumentation on network nodes and segments must be implemented to identify attempts to breach security. Some intrusion detection tools also offer automated alert, situation display, and selected response actions.

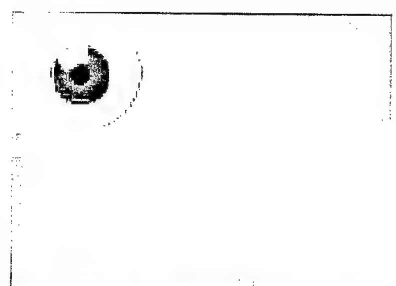


System monitoring and management are essential

- Confidentiality can be supported by use of **cryptography**—the art or science concerning the principles, means, and methods for rendering plain information unintelligible and for restoring encrypted information to intelligible form.
- A **protected distribution system (PDS)** is a wireline or fiber-optics telecommunication system that includes terminals and adequate acoustical, electrical, electromagnetic, and physical safeguards to permit its use for the unencrypted transmission of classified information. A complete protected distribution system includes the subscriber and terminal equipment and the interconnecting lines.
- Several measures can counter the threat of electronic eavesdropping. **TEMPEST** investigation, study, and equipment to control compromising emanations should be used against validated threats. **Transmission Security (TRANSEC)** measures to protect data in movement from interception and exploitation by means other than cryptanalysis include low power, directional signals, or spread-spectrum techniques that reduce adversary ability to find a signal. **Anti-tamper** mechanisms can detect alteration of the proper functioning of a security device. These technologies should be positioned on critical wide area network segments and equipment to alert managers of any damaging or destructive actions.

The kinds of enclave boundary defenses discussed in the following section can also be applied to appropriate components within the networks layer.

Technology to Defend the Enclave Boundary



Biometrics

Boundary defenses protect inside data and services from outside dangers. They also protect elements within the enclave that do not have their own self-defense capabilities. A variety of technologies can be used in combination to defend the perimeter, such as:

- **Identification and authentication** tools can recognize remote users wishing to access the enclave and control their entry. The information system analogy to challenge and response at a castle guardpost is the use of unique electronic **usernames** or **identifiers**, Personal Identification Numbers **(PIN)** or **passwords** in the form of protected or private alphanumeric strings to verify an identity and authorize access. An electronic token can validate an identity. **Biometric** mechanisms identify a person based on physical or behavioral characteristics.
- **Firewalls** implemented in hardware or software can screen out traffic based on such criteria as sender or destination address and requested service or task.

- **Malicious code and virus detectors** must be placed at the enclave perimeter to recognize unwanted harmful code and capture, monitor, or destroy it.
- **Intrusion detection** and response tools must be positioned at the boundary.
- To prevent protected information from leaving the enclave (especially, transmitting information at a higher security classification level to an enclave at a lower classification level), electronic **guards** should be installed to stop offending traffic.
- A **proxy server** can block end-user requests to access an off-limits network address. This capability is useful when such sites are known sources of malicious code or other hostile action.
- Threats to availability of enclave access to wide area networks can be controlled through appropriate **monitoring and management** mechanisms. Dynamic throttling of riskier services entering or leaving the enclave can change the system exposure in response to different INFOCONs.

Technology to Defend the Local Computing Environment

The local computing environment often contains local internal networks. Selected network protection mechanisms, such as protected distribution systems, can also be used here. In addition, effective tools must be used to extend the depth of the defense by protecting the end-systems and their internal components and associated peripheral devices.

- Providing strong control over access to components of the local computing environment protects them as well as other connected systems. Structural barriers and guard forces can block physical access by outsiders. Electronic access (often called "logical access"), should be granted only to recognized entities. Use of identified services and files must be by permission only. Mechanisms such as assignment of user accounts and privileges, **usernames**, **passwords**, **PINs**, **tokens**, and **biometrics** support electronic access control. In addition to special tools that work with operating system capabilities, applications that perform tasks (such as database management) can implement user access and privilege controls.
- To maintain confidentiality, files can be **encrypted** while in storage or transported within the enclave.
- A **digital signature** works like a handwritten signature on a paper document. In the digital signature process, a body of data (e.g., a message) is processed through an algorithm to generate a value that is unique or not easily duplicated by other means. This value is put into a special electronic digital message that is transmitted along with the original message. When the value is received, it is interpreted to verify that the original message is from the actual sender and that the original message has not been tampered with.
- Electronic **guards** can work like firewalls in reverse—to ensure that certain data does not exit via links to other elements within the enclave, or that certain services are not attempted in connections to other systems.
- **Vulnerability checkers** scan the internal nets for vulnerabilities. Other vulnerability checkers should inspect host or end-user systems. Some can repair selected vulnerabilities before they cause harm.
- **Monitoring and management** tools and **intrusion detection** tools support integrity by periodically checking the status of files and applications or alerting the administrator to suspicious indications. An audit trail record of user actions is required to allow event reconstruction to determine cause or magnitude of compromise should a security violation or malfunction occur.

- **Malicious code and virus detectors** play a vital role in maintaining integrity by recognizing and eliminating harmful software.
- **Backup** technologies automate regular copying of files and programs to enable continuity and recovery. It is vital to be able to re-start by using the last known good software configuration and data. The variety of available technologies includes emergency floppy disks with essential program files and data, on-site tape or hard disk backups, remote disk-mirroring, or operating online real-time twin systems.

The Technology Summary table below presents a representative view of how technologies relate to supported security services. The ability of specific technologies to support security services can vary when they are used alone or in combination. The characteristics of the surrounding system and security environment are important factors that influence how technologies work. It is important to note that most tools that support access control or identification and authentication also support confidentiality, availability, and integrity.

Technology Summary

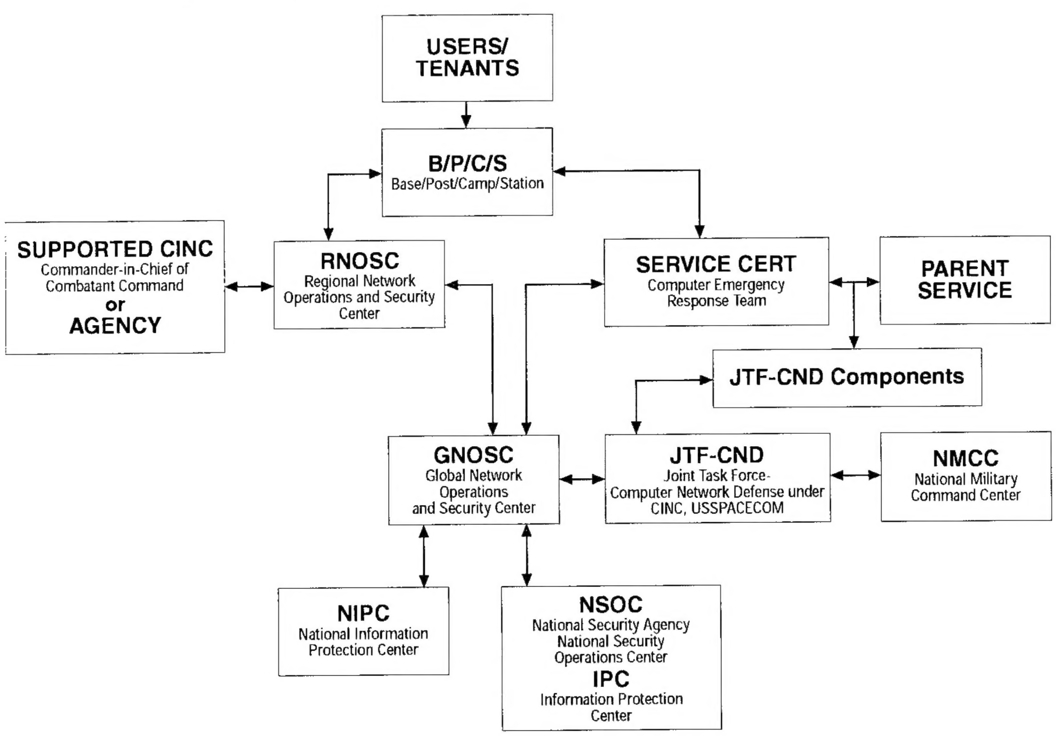
NOTE: Implementation of any combination of measures supporting a security service does NOT necessarily ensure the security service.

	Availability	Confidentiality	Integrity	Identification and Authentication	Non-Repudiation
Cryptography		○	○	○	○
User Name/ID, Password, PIN, Token, Biometrics				○	○
Digital Signatures				○	○
Firewall				○	
Intrusion Detection		○	○	○	○
Malicious Code/Virus Detection and Removal	○	○	○		
Vulnerability Checker	○	○	○	○	
Guard		○			
Proxy Server		○			
System Monitoring Tools	○		○		
TRANSEC	○	○	○		
TEMPEST		○			
Anti-tamper	○	○	○	○	
Protected Distribution Systems (PDS)	○	○	○		
Redundant/Multiple Data Paths	○		○		
Backup	○		○		○

Supporting Infrastructures

All military organizations and operations, including Information Assurance (IA), require a **logistics structure** to provide essential resources and support for maintenance, repair, and other vital services. Many of these services are common and are provided broadly across garrison and field or afloat environments. In addition, **DEFENSE IN DEPTH** requires specialized support from unique cryptographic capabilities and organized incident reporting and response.

- **Cryptography and key management infrastructures**: The cryptography function must be resourced and managed to meet all requirements at highest quality and without disclosure or theft. We must continue to design and field equipment and associated software that are reliable, fast, and secure. There must be a strong system to produce, distribute, and manage public and private keys as well as digital certificates. Efforts are in progress to improve the system by merging the current primary infrastructures for classified keys (Electronic Key Management System—EKMS) and unclassified public keys (DOD Public Key Infrastructure—DOD PKI).
- **Detection, reporting, and response infrastructures**: We must be able to discern whether an intrusion is a local, isolated event or part of a more widespread, sustained, dangerous attack. The outputs from local use of tools and intrusion detection and response actions must be delivered to organized capabilities in the chain of command. Intrusion detection information must be forwarded to specialized structures with capabilities for more sophisticated analysis and correlation of indications from a range of sources and agencies. DOD is in the process of constructing and improving a global infrastructure to manage incident reporting and enable coordinated, coherent response. Efficient operation of this infrastructure requires standardized reporting formats and procedures, automated support to transfer and analyze relevant data, and effective interface with other response capabilities.



DOD Incident Reporting and Response Structures

A Call to Action

The **DEFENSE IN DEPTH** approach will give us winning weapons against the tremendous **Information Assurance** challenges of today and the future. As the complexity and power of electronic digital computing and telecommunications increase, our forces must take full advantage of them. At the same time, adversaries of all kinds will be able to acquire and use these technologies against our critical and mission-essential capabilities.

The defense of our vital information capabilities throughout DOD requires commitment of resources, will and skill from the highest leadership to the end-user in all operational domains—land, sea, air, and space. The full array of DOD elements—that includes the CINCs (commanders in chief of combatant commands), Military Departments and Services, and DOD agencies—must plan and execute powerful and integrated Information Assurance (IA) operations.

We must maximize the contributions of certified expert people, disciplined operations that follow policies and apply successful procedures, and proven reliable technology solutions. In these efforts, the ***human factor is and will continue to be essential***—it takes people to make and use technologies and conduct IA operations. ***DEFENSE IN DEPTH depends on each of us***. We must master new technologies, remain on watch for new and changing threats and vulnerabilities, and continue vigorous efforts to build a formidable Information Assurance **DEFENSE IN DEPTH.**

When medieval realms were invaded, they often relied on a network of interconnected castles and fortified towns to provide mutual support through counterattacks and reinforcements.

A castle under siege was usually outnumbered by the adversary. Thus, defenders depended upon the mutually supporting combination of all the defensive resources at hand in the castle to achieve maximum combat power.

These Internet sites are valuable starting points for further information and references to additional sources:

- Extranet for Security Professionals (ESP)—http://isp.hpc.org or http://www.xsp.org
- Information Assurance Technical Framework Forum (IATFF, formerly Network Security Framework Forum NSFF)—http://www.nsff.org
- U.S. Air Force Departmental Publishing Office (AFDPO/PP)—http://afpubs.hq.af.mil
- U.S. Army Publications Agency (USARPA), USAPA Electronic Publications and Forms—http://www.usapa.army.mil/gils
- U.S. Dept. of Commerce, National Institute of Standards and Technology (NIST) Computer Security Division of Information Technology Laboratory—http://www.itl.nist.gov/div893
- U.S. Dept. of Defense Computer Emergency Response Team (DOD-CERT)—http://www.cert.mil
- U.S. Dept. of Defense, Defense Information Systems Agency (DISA) Information Assurance Support Environment (IASE)—http://mattche.iiie.disa.mil
- U.S. Dept. of Defense, Defense Security Service (DSS)—http://www.dss.mil/index.htm
- U.S. Dept. of Defense, National Security Agency (NSA) Information Systems Security Organization (ISSO)—http://www.nsa.gov:8080/isso/index.html
- U.S. Dept. of Defense, Washington Headquarters Services Directives And Records Branch (DOD directives, instructions, regulations, etc.)—http://web7.whs.osd.mil/corres.htm
- U.S. Dept. of Defense, The Joint Staff, Joint Electronic Library (doctrine, DOD Dictionary, etc.)—http://www.dtic.mil/doctrine/jel/index.html
- U.S. Federal Computer Incident Response Capability (FEDCIRC)—http://www.fedcirc.gov
- U.S. National Security Telecommunications and Information Systems Security Committee (NSTISSC)—http://constitution.ncsc.mil/wws/nstissc
- U.S. National Infrastructure Protection Center (NIPC)—http://www.nipc.gov
- U.S. Navy Electronic Directives System (NEDS)—http://neds.nebt.daps.mil
- U.S. Navy INFOSEC site—http://infosec.nosc.mil/content.html

I WANT YOU for INFORMATION ASSURANCE